NSE4_FGT-6.2 Q&As

Fortinet NSE 4 - FortiOS 6.2

Pass Fortinet NSE4_FGT-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse4_fgt-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

When using SD-WAN, how do you configure the next-hop gateway address for a member interface so that FortiGate can forward Internet traffic?

A. It must be configured in a static route using the sdwan virtual interface.

B. It must be provided in the SD-WAN member interface configuration.

C. It must be configured in a policy-route using the sdwan virtual interface.

D. It must be learned automatically through a dynamic routing protocol.

Correct Answer: A

QUESTION 2

Examine this output from a debug flow: Which statements about the output are correct? (Choose two.)

```
id=2 line=4677 msg= "vd-root received a packet (photo =6, 66.171.121.44:80-
>10.200.1.1:49886) from port1. flag [S.], seg 3567496940, ack 2176715502, win
5840"
id=2 line= 4739 msg= "Find an existing session, id-00007fc0, reply direction"
id=2 line= 2733 msg "DNAT 10.200.1.1:49886->10.0.1.10:49886"
id=2 line=2582 msg= "find a route: flag= 00000000 gw-10.0.1.10 via port3"
```

A. FortiGate received a TCP SYN/ACK packet.

B. The source IP address of the packet was translated to 10.0.1.10.

C. FortiGate routed the packet through port 3.

D. The packet was allowed by the firewall policy with the ID 00007fc0.

Correct Answer: AC

QUESTION 3

A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not.

Which configuration option is the most effective way to support this request?

A. Implement web filter authentication for the specified website.

B. Implement a web filter category override for the specified website.

C. Implement DNS filter for the specified website.

D. Implement web filter quotas for the specified website.

Correct Answer: B

QUESTION 4

Which of the following statements about converse mode are true? (Choose two.)

A. FortiGate stops sending files to FortiSandbox for inspection.

B. FortiGate stops doing RPF checks over incoming packets.

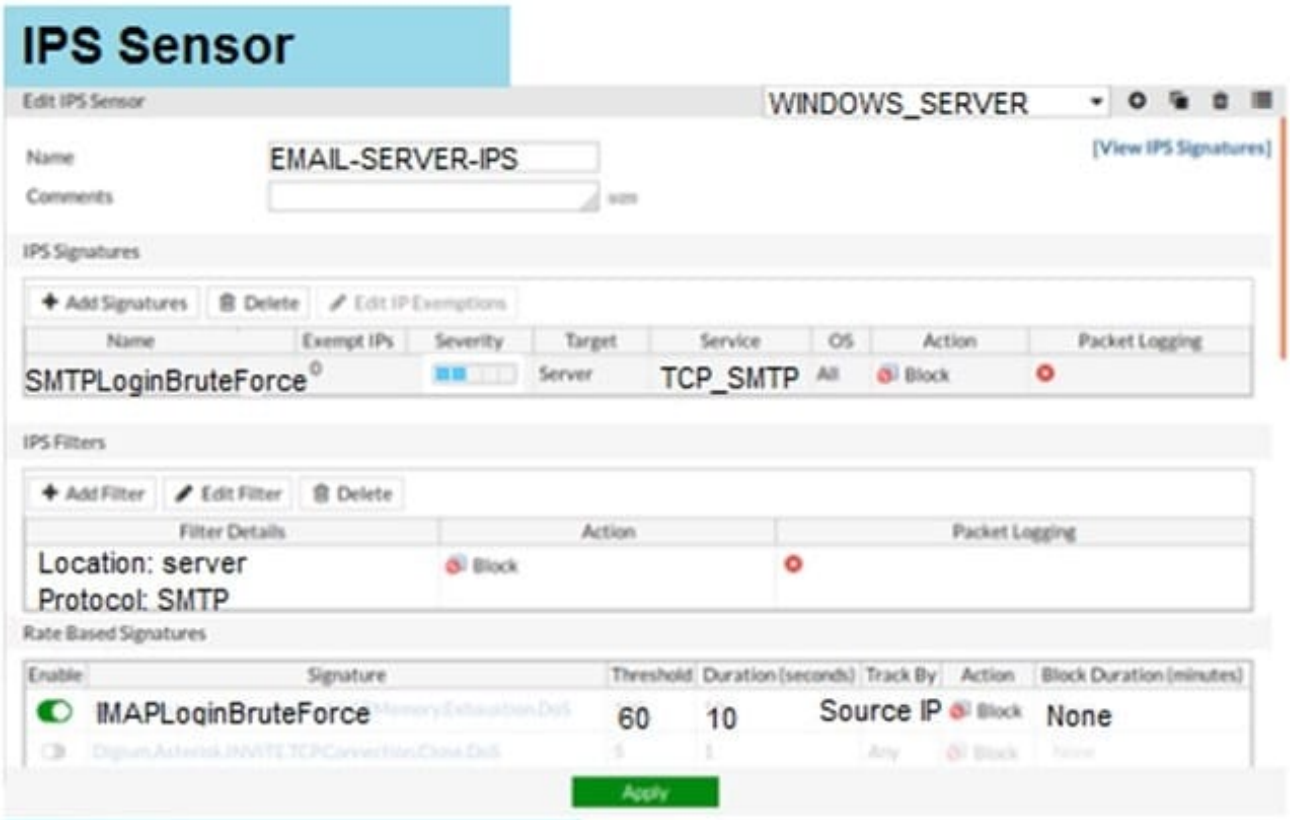
C. Administrators cannot change the configuration.

D. Administrators can access the FortiGate only through the console port.

Correct Answer: AC

QUESTION 5

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. SMTP.Login.Brute.Force

B. IMAP.Login.brute.Force

C. ip_src_session

D. Location: server Protocol: SMTP

Correct Answer: B

QUESTION 6

Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.

B. Source IP is translated to the outgoing interface IP.

C. Connections are tracked using source port and source MAC address.

D. Port address translation is not used.

Correct Answer: AB

QUESTION 7

Which of the following conditions are required for establishing an IPSec VPN between two FortiGate devices? (Choose two.)

A. If XAuth is enabled as a server in one peer, it must be enabled as a client in the other peer.

B. If the VPN is configured as route-based, there must be at least one firewall policy with the action set to IPSec.

C. If the VPN is configured as DialUp User in one peer, it must be configured as either Static IP Address or Dynamic DNS in the other peer.

D. If the VPN is configured as a policy-based in one peer, it must also be configured as policy-based in the other peer.

Correct Answer: BC

QUESTION 8

An administrator is running the following sniffer command:

diagnose sniffer packet any "host 10.0.2.10" 3

What information will be included in the sniffer output? (Choose three.)

A. IP header

B. Ethernet header

C. Packet payload

D. Application header

E. Interface name

Correct Answer: ABC

QUESTION 9

Which of the following statements about the FSSO collector agent timers is true?

A. The workstation verify interval is used to periodically check if a workstation is still a domain member.

B. The IP address change verify interval monitors the server IP address where the collector agent is installed, and the updates the collector agent configuration if it changes.

C. The user group cache expiry is used to age out the monitored groups.

D. The dead entry timeout interval is used to age out entries with an unverified status.

Correct Answer: D

QUESTION 10

Which of the following statements are true when using WPAD with the DHCP discovery method? (Choose two.)

A. If the DHCP method fails, browsers will try the DNS method.

B. The browser needs to be preconfigured with the DHCP server\\'s IP address.

C. The browser sends a DHCPINFORM request to the DHCP server.

D. The DHCP server provides the PAC file for download.

Correct Answer: AC

QUESTION 11

Examine this FortiGate configuration: How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

A. It always authorizes the traffic without requiring authentication.

B. It drops the traffic.

C. It authenticates the traffic using the authentication scheme SCHEME2.

D. It authenticates the traffic using the authentication scheme SCHEME1.

Correct Answer: D

QUESTION 12

An administrator is attempting to allow access to https://fortinet.com through a firewall policy that is configured with a web filter and an SSL inspection profile configured for deep inspection. Which of the following are possible actions to eliminate the certificate error generated by deep inspection? (Choose two.)

A. Implement firewall authentication for all users that need access to fortinet.com.

B. Manually install the FortiGate deep inspection certificate as a trusted CA.

C. Configure fortinet.com access to bypass the IPS engine.

D. Configure an SSL-inspection exemption for fortinet.com.

Correct Answer: AD

QUESTION 13

An administration wants to throttle the total volume of SMTP sessions to their email server. Which of the following DoS sensors can be used to achieve this?

A. tcp_port_scan

B. ip_dst_session

C. udp_flood

D. ip_src_session

Correct Answer: A

QUESTION 14

On a FortiGate with a hard disk, how can you upload logs to FortiAnalyzer or FortiManager? (Choose two.)

A. hourly

B. real time

C. on-demand

D. store-and-upload

Correct Answer: BD

QUESTION 15

A FortiGate device has multiple VDOMs. Which statement about an administrator account configured with the default prof_admin profile is true?

A. It can create administrator accounts with access to the same VDOM.

B. It cannot have access to more than one VDOM.

C. It can reset the password for the admin account.

D. It can upgrade the firmware on the FortiGate device.

Correct Answer: A